

# Secure Routing for Multi-Hop Ad Hoc Networks with Inhomogeneous Eavesdropper Clusters

Gaojie Chen, *Member, IEEE*, Justin P. Coon *Senior Member, IEEE* and Shahriar E. Tajbakhsh

**Abstract**—This paper studies finding the secure path according to the secrecy connectivity probability (SCP) in the multi-hop ad hoc networks in the presence of inhomogeneous eavesdropper clusters. We consider both random and fixed eavesdropper clusters, where the former case assumes that there is no knowledge of the locations of the clusters and the latter case assumes that the locations of the clusters can be estimated accurately. Firstly, we derive the end-to-end SCP to characterize the secrecy performance of a given path in a general multi-hop wireless network with half-duplex (HD) randomize-and-forward relaying. Then we consider a full-duplex (FD) scheme at the legitimate receiver, which receives the useful information while broadcasting a jamming signal to the potential eavesdroppers to further enhance the secrecy connectivity. Then, a novel secure routing algorithm which can provide the maximum SCP for any legitimate transmitter/receiver pair in a distributed manner is proposed. The theoretical analysis is verified by Monte Carlo simulation results. The results show that our secure routing algorithm provides similar results compared to an exhaustive search. For the random eavesdropper cluster case, the optimal route is independent of the knowledge of the cluster, which is the same as the homogeneous eavesdropper case. However, for the case where eavesdropper clusters are fixed and their locations are known *a priori*, the optimal path selection depends on the radii and locations of the eavesdropper clusters and the average number of eavesdroppers in each cluster.

**Index Terms**—Multi-hop ad hoc networks, Physical layer security, stochastic geometry, full-duplex, routing algorithm

## I. INTRODUCTION

### A. Background

The concept of wireless ad hoc networks refers to the network model where devices directly transmit information signals to each other by utilizing point-to-point channels without using centralized infrastructure. Furthermore, because communications in wireless ad hoc networks frequently happen over unlicensed spectrum by utilizing existing short-range wireless communications technologies, the interference between cellular and ad hoc networks can be avoided [1]. Therefore, wireless ad hoc networks promise to serve as a

potential technique for the wireless networks in many applications, such as 5G, public safety and military systems.

Traditional security has been focused on the higher layers of communication networks, rather than the physical layer. For data confidentiality, encryption is the primary scheme of ensuring secrecy, which works well in most current systems. However, in some emerging networking architectures, issues of key management or computational complexity cause the implementation of data encryption to be difficult [2], [3]. For example, for ad hoc networks, with the number of devices involved, information may be transmitted through many intermediate nodes from the source to the destination, which increases the probability of losing a key [2]. Therefore, how to protect the transmission security in ad hoc networks becomes a crucial issue. In order to deal with this issue, physical layer security (PLS) has been widely utilized for secure data transmission by considering the physical properties of the radio channel based on Shannon theory. For example, when the capacity of the intended data transmission channel is larger than that of the eavesdropping channel, the information can be sent at a rate close to the *secrecy capacity*, which is the difference between the data transmission channel capacity and eavesdropping channel capacity, so that only the legitimate receiver can successfully retrieve the information. In order to enhance secrecy performance, many schemes have been implemented, i.e., beamforming, buffer-added relay, artificial noise and the full-duplex (FD) jamming, etc. However, from the efficient implementation perspective, with the development of FD antenna design, the FD jamming scheme has been considered widely to improve the secrecy performance [4], [5]. Therefore, this paper exploits the FD jamming relay to further enhance the secrecy performance.

Furthermore, due to the passive nature of eavesdroppers, the exact locations of eavesdroppers may not be obtained by the legitimate node. In order to consider the uncertainty of eavesdropper locations, in 2008, a powerful scheme to model the randomly located eavesdroppers in large scale networks was provided by [6], [7], in which the nodes may spread out across the area, which is an analytically convenient and reasonable assumption for homogeneously located nodes in wireless networks. Mathematically, the assumption in that work is that the node positions can be modeled as a homogeneous (or stationary) Poisson point process (PPP). While the PPP may be a good model for certain systems, it is highly likely that the distribution of locations of nodes is not uniform, for example, some users are either clustered or more regularly distributed. Furthermore, even if the complete set of nodes constitutes a PPP, the subset of active nodes may not be

This work was supported by EPSRC grants number EP/N002350/1 (“Spatially Embedded Networks”) and EP/R006377/1 (“M3NETs”).

Copyright (c) 2015 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

G. Chen is with the Department of Engineering, University of Leicester, Leicester, LE1 7RH, U.K., Email: gaojie.chen@leicester.ac.uk.

J. P. Coon and S. E. Tajbakhsh are with the Department of Engineering Science, University of Oxford, Parks Road, Oxford, UK, OX1 3PJ, Emails: {justin.coon and shahriar.etemaditajbakhsh}@eng.ox.ac.uk.

homogeneously Poisson [8], [9]. Certainly, it is suitable that sentries in a sensor network and simultaneous transmitters in a wireless ad hoc network ([10] and [11]) form more regular processes to maximize coverage and spatial reuse, respectively. Moreover, the clustered processes have been considered in many academic papers [8]–[15]. For example, the clustering of eavesdropper nodes may be due to geographical factors, i.e., communicating users in a building or groups of nodes moving in a coordinated fashion, which can be modeled by geographical clustering. Therefore, this motivates us to consider extending the rich set of results available for PPPs to other node distributions, i.e., Poisson cluster process (PCP), in the context of secure routing based on PLS.

### B. Related Work

Based on information-theoretic security, recently, PLS in cooperative relay networks has been investigated widely [4], [14], [16]–[21]. In fact, cooperative networks not only enlarge the coverage area of transmission, but also provide diversity and coding gains for system performance improvement. The relay nodes also act as friendly jammers to generate jamming signals to destroy the channels of the eavesdroppers. In [16], the proposed scheme enabled a relay selection scheme to improve secrecy performance against eavesdroppers. The authors in [17] enhanced the security performance between the transmitter and receiver by using multiple cooperating relays, which employ amplify-and-forward (AF), decode-and-forward (DF), and cooperative jamming (CJ). The authors in [18] investigated the optimal location of the relay to achieve secrecy connectivity for DF and randomize-and-forward (RaF) relaying scenarios. In [14], the diversity orders and intercept probability expressions of optimal AF and DF relay selection were obtained. Furthermore, a multiple-input multiple-output (MIMO) technique was considered in the context of secure communications in [19] and [20], which further increases secrecy capacity and improves the reliability of the system. The authors in [21] considered the secure transmission in buffer-aided DF relay networks with the max-ratio relay selection. The full-duplex jamming relay was provided to enhance the secrecy outage probability in [4].

However, these papers considered a small number of nodes, and assumed that the channel state information (CSI) and/or exact locations of eavesdroppers are available at the legitimate node. It is not realistic to know the exact locations of eavesdroppers in practice. Therefore, the impacts of random eavesdroppers' locations on the system security have been studied [22]–[28]. Location distributions of passive eavesdroppers can be described accurately by utilizing the Poisson point process (PPP) or binomial point process (BPP), therefore, [22] modeled the locations of transmitters and eavesdroppers as two independent two-dimensional PPPs, and studied the secrecy capacity in mobile communication networks. Then, MIMO with a beamforming transmission scheme was utilized in [23], [24] to enhance the security of the system. To further enhance the system security, the artificial noise was exploited against randomly distributed eavesdroppers in [25], [26]. Beamforming was also implemented to improve the secrecy performance

in visible light communications in [29], [30]. However, the complexity of the implementation is significantly increased by utilizing multiple transmitters/antennas with beamforming. Thus, in [27], [28], the transmit antenna selection scheme was considered as an alternative to beamforming technology, which not only improves the secrecy performance, but also enhances the system reliability.

Most of the literature, however, focuses on the two hop scenario, leaving the design of secure routing in ad hoc networks as an open question. Although there exist some works on secure routing, such as [31], [32], some challenges or shortcomings still need to be addressed. For example, the CSI and exact locations of the eavesdroppers can be obtained at the legitimate nodes, which is usually impractical, was assumed in [31]. Therefore, [32] investigated the secure routing scheme in ad hoc networks with a homogeneous eavesdropper spatial location. Their results point to the intuitively satisfying (and somewhat obvious) conclusion that the routing path following the straight line between the legitimate source and destination is always optimal. However, as [8]–[10] mentioned that the location of node is not completely uniformly distributed. Therefore, for clustered eavesdropper scenario, finding the optimal path that maximizes the secrecy connectivity probability (SCP) is still an open problem. Therefore, a secure routing algorithm based on the SCP in wireless ad hoc networks with inhomogeneous (both random and fixed location) eavesdropper clusters will be proposed in this work. Moreover, the proposed secure routing algorithm can be easily utilized in public safety and military applications when some areas are potentially unsafe. Furthermore, full-duplex (FD) scheme is an attractive alternative to enhance the security in PLS because the self-interference can be cancelled to achieve the noise floor by utilizing the recent signal processing and antenna design methods [33]. Thus, to improve secrecy connectivity, the FD scheme at the receiver will be considered in our work. The contributions of the paper are as follows:

- We derive the exact expressions and lower bound of SCP for half-duplex (HD) legitimate receivers based on the RaF scheme for a given path in the presence of multiple inhomogeneous (both random and fixed) eavesdropper clusters.
- We propose an FD scheme at the legitimate receivers to enhance the SCP and obtain the exact expressions for the SCP.
- We propose a secure routing algorithm by using two approximate metrics to find the sub-optimal route from the source to the destination in a distributed way.
- We verify the theoretical analysis and illustrate the proposed secure routing algorithm by utilizing Monte Carlo simulations and numerical results. The results give useful insight for designing practical secure ad hoc networks based on different system parameters.

The rest of this paper is organized as follows. In Section II, we provide the system model and problem formulation. Then we analyze SCP for a given path with random eavesdropper clusters in Section III. Section IV analyzes the SCP by using HD and FD forwarding schemes at the legitimate receiver for

Table I  
NOTATION AND SYMBOLS USED IN THE PAPER

Symbol	Explanation and Definition
$\alpha$	path loss exponent
$\mathbb{R}^2$	two-dimensional space
$N_{C_k}$	the average number of ED in cluster $C_k$
$\mathbb{E}[\cdot]$	expectation operation
$\max_{k \in \{1, \dots, K\}} (x_k)$	maximum function with a set
$\ \cdot\ $	distance operation
$\mathbb{P}(\cdot)$	probability operator
$\mathbb{Z}^+$	positive real numbers
$\mathcal{O}(x)$	big $\mathcal{O}$ notation
$E_1(x)$	exponential integral function $E_1(x) = \int_x^\infty \frac{e^{-t}}{t} dt$
R.V.	random variable

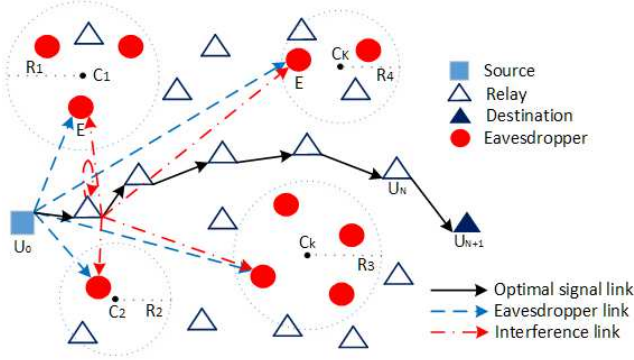


Figure 1. The wireless ad hoc networks in the presence of inhomogeneous eavesdropper clusters.

a given path with fixed eavesdropper clusters, respectively. In Section V, we propose the secure routing algorithm to select optimal path having the maximum SCP for different scenarios. Then, numerical simulations are provided to verify the analysis in Section VI. Finally, Section VII concludes the paper. The notation and symbols mentioned in the work are listed in Table I.

## II. SYSTEM MODEL AND PROBLEM FORMULATION

### A. System Model

In this section, we focus on a secure transmission between the source ( $U_0$ ) and the destination ( $U_{N+1}$ ) by utilizing a number of trusted RaF<sup>1</sup> relays ( $U_i$ ,  $i \in (1, 2, \dots, N)$ ) so that the combination of two received signal cannot help to recover the secure message if the signal in each hop is irrecoverable [34] (see Fig. 1). To be specific, we assume the source, relay<sup>2</sup> and EDs are equipped with HD antennas so that they cannot transmit and receive simultaneously. Furthermore, the worse case scenario where the spatial locations of eavesdroppers change independently for every time slot  $t$ ,  $t \in (t = 0, 1, \dots, N)$  and all of the eavesdroppers can

<sup>1</sup>RaF strategy requires that the source and the relays utilize different codebooks with independent randomness, and the source (relay) uses the well-known Wyner wiretap code at different transmission time slots.

<sup>2</sup>In order to enhance SCP, in the Section IV, we consider an FD receiver, which means the receiver simultaneously receives the useful information and sends a jamming signal to disrupt eavesdropping signal.

share the eavesdropping information, which is termed the *colluding scenario*, is considered.

Without loss of generality, the locations of the source and the destination are fixed. In our paper, we consider both random and fixed eavesdropper clusters. For the former case, the locations of eavesdroppers are modeled as a stationary and isotropic Poisson cluster process (PCP)  $\Phi_E$  on  $\mathbb{R}^2$ . Then we assume the centers of eavesdropper clusters form a stationary Poisson point process  $\Phi_C$  with intensity  $\lambda_C$  and therefore the intensity of the eavesdropper cluster process is  $\lambda_E = \lambda_C N_E$ , where  $N_E$  is the average number of the eavesdroppers in the representative cluster. For the latter case, the locations of eavesdropping clusters can be estimated as potentially unsafe areas. The exact method of performing this estimation is not explicitly considered here. Then we consider the case where eavesdropper locations are modeled as a stationary and isotropic Poisson process  $\Phi_{C_k}$  in  $K$  clusters with radii  $R_{C_k}$  ( $k \in (1, 2, \dots, K)$ ) and average numbers of eavesdroppers  $N_{C_k}$  ( $k \in (1, 2, \dots, K)$ ). In other words, cluster centres of eavesdroppers are fixed, but eavesdropper numbers and positions within these clusters follow a uniform distribution in a circle with radius  $R$ , therefore, the density function can be obtained by

$$f(x_e) = \begin{cases} \frac{1}{\pi R^2}, & \text{if } \|x_e\| \leq R, \\ 0, & \text{otherwise.} \end{cases} \quad (1)$$

In this paper, we assume all wireless channels undergo path loss and independent Rayleigh fading channels, which is given by  $h_{ij} = \rho_{ij} d_{ij}^{-\alpha/2}$ , where  $d_{ij}$  and  $\alpha$  denote the distance between node  $i$  and  $j$ , and the pathloss exponent, respectively. The channel coefficient  $\rho_{ij}$  is a complex Gaussian random variable with unit variance. Thus, the corresponding channel gains  $|h_{ij}|^2$  are exponentially independently distributed with mean  $\lambda_{ij}$ , and the average channel power is defined as  $\lambda_{ij} = \mathbb{E}[|h_{ij}|^2] = d_{ij}^{-\alpha}$ .

### B. Secrecy Connectivity Probability

Firstly, the SCP of wireless wiretap system with RaF relays in the presence of random eavesdropper clusters is derived in this subsection. We assume that the CSI between the source and relays are known by each other and the signal transmission is achieved by using the time division multiple access (TDMA)<sup>3</sup>. We suppose that the message  $x$  from node  $U_i$  can be received at the latter node  $U_{i+1}$  and ED. Thus, the received signal at the  $U_{i+1}$  and ED are given by:

$$y_{i,i+1}(t) = \sqrt{P_B} \frac{h_{i,i+1}(t)}{d_{i,i+1}^{\alpha/2}} x(t) + n_{i+1}(t), \quad (2)$$

$$y_{i,e}(t) = \sqrt{P_B} \frac{h_{i,e}(t)}{d_{i,e}^{\alpha/2}} x(t) + n_e(t) \quad (3)$$

where  $P_B$  represents the transmit power of the transmitter, and  $n_{i+1}$  and  $n_e$  denote the additive white Gaussian noise

<sup>3</sup>By using the TDMA protocol, the system delay is equivalent to the number of the TDMA slots, which depends on the number of selected relay nodes in the optimal path. For the machine type IoT system, devices may directly attempt to access the same destination using the same resources, which leads to a congestion problem. However, the issue of collision mitigation is beyond of the scope of this paper.

(AWGN) with variance  $\sigma_n^2$  at nodes  $U_{i+1}$  and ED, respectively. For notational convenience, the time index  $t$  is ignored below unless otherwise noted necessary. Then the capacity of  $U_{i+1}$  and the total capacity of the eavesdropper is given as:

$$C_{i,i+1} = \log_2 \left( 1 + \frac{P_B |h_{i,i+1}|^2}{\sigma_n^2 d_{i,i+1}^\alpha} \right), \quad (4)$$

$$C_{i,E} = \log_2 \left( 1 + \sum_{e \in \Phi_E} \left( \frac{P_B |h_{i,e}|^2}{\sigma_n^2 d_{i,e}^\alpha} \right) \right). \quad (5)$$

Note that in (5), since we consider the colluding eavesdroppers as the worst case scenario from the secrecy point of view, all signals received by the eavesdropper will be combined. Furthermore, we assume the spatial locations of eavesdroppers vary independently at every time slot and we consider the RaF relay scenario, therefore, the SCP is defined as [34]

$$P = \prod_{i=1}^N \mathbb{P}(C_{i,i+1} - C_{i,E} > 0) \\ = \begin{cases} \prod_{i=1}^N \mathbb{P} \left( \frac{|h_{i,i+1}|^2 d_{i,i+1}^{-\alpha}}{\sum_{e \in \Phi_E} (|h_{i,e}|^2 d_{i,e}^{-\alpha})} > 1 \right) \\ \text{for random eavesdropper cluster,} \\ \prod_{i=1}^N \mathbb{P} \left( \frac{|h_{i,i+1}|^2 d_{i,i+1}^{-\alpha}}{\sum_{k=1}^K \sum_{e \in \Phi_{C_k}} (|h_{i,e}|^2 d_{i,e}^{-\alpha})} > 1 \right) \\ \text{for fixed eavesdropper cluster.} \end{cases} \quad (6)$$

### III. SCP FOR A GIVEN PATH WITH RANDOM EAVESDROPPER CLUSTERS

In this section, we consider the random eavesdropper clusters scenario, where the eavesdroppers are randomly distributed in the infinite area based on a PCP with intensity function  $\lambda_E$ . Thus, the SCP between  $U_i$  and  $U_{i+1}$  is given by

$$P_i = \mathbb{P} \left( \frac{|h_{i,i+1}|^2 d_{i,i+1}^{-\alpha}}{\sum_{e \in \Phi_E} (|h_{i,e}|^2 d_{i,e}^{-\alpha})} > 1 \right) \\ = \mathbb{E}_{e \in \Phi_E} \left[ \prod_{e \in \Phi_E} e^{-|h_{i,e}|^2 d_{i,e}^{-\alpha} d_{i,i+1}^\alpha} \right] \\ \stackrel{(a)}{=} \mathbb{E}_{e \in \Phi_E} \left[ \prod_{e \in \Phi_E} \int_0^\infty e^{-t d_{i,e}^{-\alpha} d_{i,i+1}^\alpha} e^{-t} dt \right] \\ = \mathbb{E}_{e \in \Phi_E} \left[ \prod_{e \in \Phi_E} \frac{1}{1 + d_{i,i+1}^\alpha d_{i,e}^{-\alpha}} \right] \\ \stackrel{(b)}{=} \exp \left[ -\lambda_C \int_{\mathbb{R}^2} \left[ 1 - \mathcal{M} \left( \int_{\mathbb{R}^2} \frac{f(x_e)}{1 + d_{i,i+1}^\alpha d_{i,e}^{-\alpha}} dx_e \right) \right] dx_c \right] \quad (7)$$

where we let  $t = |h_{i,e}|^2$  and the probability density function (PDF) of  $t$  is  $e^{-t}$  in (a), and (b) holds for Neyman-Scott cluster process by utilizing the probability generating functional (PGF) [35] and

$$\mathcal{M}(z) = \exp(-N_E(1-z)) \quad (8)$$

when the number of eavesdroppers in the representative cluster is Poisson distributed with mean  $N_E$ . It is impossible to derive

a closed-form expression of (7), but we can get a lower bound on (7), which is given by Lemma 1.

*Lemma 1:* The SCP between any two legitimate nodes with random eavesdropper clusters is lower bounded by

$$P_{co,i}^{(G)} \geq \exp \left( -\pi \lambda_E \frac{d_{i,i+1}^2}{\text{sinc}(2/\alpha)} \right). \quad (9)$$

*Proof:* More detail in Appendix A. ■

*Remark 1:* For given  $d_{i,i+1}$ , the SCP for the random eavesdropper clusters case is related to the intensity of eavesdroppers  $\lambda_E$  and the path loss exponent  $\alpha$ . It can be obviously shown that the SCP of PCPs can be higher than that of PPPs (9) with the same intensity of eavesdroppers. More details of effects of these parameters on system performance are given in Section VI.

Substituting (9) into (6), the lower bound on the SCP can be obtained as

$$P_i \geq \exp \left( -\frac{\pi \lambda_E \sum_{i=0}^{N-1} d_{i,i+1}^2}{\text{sinc}(2/\alpha)} \right). \quad (10)$$

In the same scenarios, we may have the knowledge of the eavesdropping cluster, i.e., the potentially unsafe areas. In the next section, we will investigate this case.

### IV. SCP FOR A GIVEN PATH WITH FIXED EAVESDROPPER CLUSTERS

Due to geographical limitations, the inhomogeneously distributed eavesdroppers can be modelled by using geographical clustering [10], for example, eavesdroppers are in a building or groups of nodes moving in a coordinated fashion. Furthermore, some areas can be easily distinguished as potentially unsafe areas<sup>4</sup>, therefore, we can estimate the location and radius of clusters and the number of clusters as well as the average number of eavesdroppers per cluster. The question of how to calculate the SCP with the partial knowledge of eavesdropper locations is the focus of this section. Specifically, we study a practical scenario based on the characteristics of the SCP with the knowledge of eavesdroppers' cluster.

#### A. The SCP based on HD Receiver

Since the locations and radii of eavesdropper's cluster are known, the SCP between  $U_i$  and  $U_{i+1}$  for HD receiver is given by (11) at the top of the next page, where (a) holds by using the PGF lemma proposed in [35],  $d_{i,e} = \sqrt{d_{i,k}^2 + r^2 - 2\cos(\theta)rd_{i,k}}$ , and  $d_{i,k}$  denotes the distance between the  $U_i$  and the center of cluster  $K$ . Eq. (11) can be calculated by using standard numerical integration techniques for given sets of parameters. For the case when  $\alpha = 2$ , the exact result can be simplified to be (12) at the top of the next page.

*Remark 2:* For fixed  $d_{i,i+1}$ , the SCP depends on the average number of eavesdroppers in each representative cluster, but also the related information of each cluster, i.e. the radius and

<sup>4</sup>For example, we can easily find the location of commercial rivals or uncertain area with a high floating population.

$$\begin{aligned}
P_i^{(H)} &= \mathbb{P} \left( \frac{|h_{i,i+1}|^2 d_{i,i+1}^{-\alpha}}{\sum_{k=1}^K \sum_{e \in \Phi_{C_k}} (|h_{i,e}|^2 d_{i,e}^{-\alpha})} > 1 \right) = \mathbb{E}_{e \in \Phi_{C_k}} \left[ \exp \left( -d_{i,i+1}^\alpha \sum_{k=1}^K \sum_{e \in \Phi_{C_k}} (|h_{i,e}|^2 d_{i,e}^{-\alpha}) \right) \right] \\
&= \prod_{k=1}^K \mathbb{E}_{e \in \Phi_{C_k}} \left[ \prod_{e \in \Phi_{C_k}} \exp(-d_{i,i+1}^\alpha d_{i,e}^{-\alpha} |h_{i,e}|^2) \right] = \prod_{k=1}^K \mathbb{E}_{e \in \Phi_{C_k}} \left[ \prod_{e \in \Phi_{C_k}} \frac{1}{1 + d_{i,i+1}^\alpha d_{i,e}^{-\alpha}} \right] \\
&\stackrel{(a)}{=} \prod_{k=1}^K \exp \left[ -\frac{N_{C_k}}{\pi R_{C_k}^2} \int_0^{2\pi} \int_0^{R_{C_k}} \left( \frac{d_{i,e}^{-\alpha} d_{i,i+1}^\alpha}{d_{i,e}^{-\alpha} d_{i,i+1}^\alpha + 1} \right) dr d\theta \right]
\end{aligned} \tag{11}$$

$$P_i^{(H)} = \prod_{k=1}^K \exp \left( -\frac{N_{C_k} d_{i,i+1}^2}{R_{C_k}^2} \ln \left( \frac{R_{C_k}^2 - d_{i,k}^2 + d_{i,i+1}^2 + \sqrt{R_{C_k}^4 + 2R_{C_k}^2 (d_{i,i+1}^2 - d_{i,k}^2) + (d_{i,i+1}^2 + d_{i,k}^2)^2}}{d_{i,i+1}^2 + 2} \right) \right) \tag{12}$$

location. These parameters can be considered for the optimal path selection when determining the best configuration for achieving a SCP. More details about the trade-off between these parameters on security performance is provided in Section VI.

Finally, substituting (11) into (6), the end-to-end SCP for HD receiver is given by

$$P^{(H)} = \prod_{i=1}^N P_i^{(H)}. \tag{13}$$

### B. The SCP Enhancement by Using FD Receiver

In this subsection, in order to enhance the SCP, we consider an FD receiver which not only receives the signal, but also generates the jamming signal to the eavesdropper. We assume that the residual self-interference (SI) can be reduced to noise floor by using the SI cancellation scheme in [36]<sup>5</sup>. Then the SCP with the FD receiver between  $U_i$  and  $U_{i+1}$  is given by<sup>6</sup> (14) at the top of the next page, where in (a) we let

$$l = \frac{d_{i,i+1}^\alpha d_{i,e}^{-\alpha} |h_{i,e}|^2}{\gamma_{C_k} |h_{i+1,e}|^2 d_{i+1,e}^{-\alpha} + 1}$$

and the PDF of  $l$  is

$$f_L(l) = \frac{e^{-\frac{l}{\Psi}} (\Psi \Omega + \Omega l + \Psi)}{(\Psi + \Omega l)^2}$$

(b) holds by the PGF lemma,  $\Psi = d_{i,i+1}^\alpha d_{i,e}^{-\alpha}$ ,  $\Omega = \gamma_{C_k} d_{i+1,e}^{-\alpha}$  and  $\gamma_{C_k}$  denotes the jamming-to-noise power ratio. Fig. 2 gives the distance between  $U_i$ ,  $U_{i+1}$  and  $E_{k,e}$  by using the law of cosines, which are given as

$$\begin{aligned}
d_{i,e} &= \sqrt{d_{i,k}^2 + r^2 - 2\cos(\theta)rd_{i,k}} \\
d_{i+1,e} &= \sqrt{d_{i+1,k}^2 + r^2 - 2\cos(\theta + \theta_c)rd_{i+1,k}} \\
\theta_c &= \arccos \left( \frac{d_{i,k}^2 + d_{i+1,k}^2 - d_{i,i+1}^2}{2d_{i,k}d_{i+1,k}} \right)
\end{aligned}$$

where  $d_{i+1,k}$  denotes the distance between  $U_{i+1}$  and the center of cluster  $K$ . Note that (14) can be evaluated for given sets of parameters by using standard numerical integration techniques or software. Meanwhile, according to [37],  $e^x \mathbf{E}_1(x)$  can be bounded by elementary functions as follows:

$$\frac{1}{x+1} < e^x \mathbf{E}_1(x) \stackrel{(a)}{\leq} \frac{1}{x} \quad \text{if } x > 0 \tag{15}$$

where the equality of (a) holds when  $x \gg 1$ . Therefore, for (14), when the jamming power-to-noise ratio is small so that  $\Omega$  is smaller than  $\Psi + 1$ , we can use the upper bound (a) of (15) to get a lower bound on SCP, which converges to the HD case given in (11). When the jamming power-to-noise ratio is large,  $\Omega$  is greater than  $\Psi + 1$ , the lower bound of (15) can be utilized to derive the upper bound of SCP as

$$P_i^{(F)} < \prod_{k=1}^K \exp \left[ -\frac{N_{C_k}}{\pi R_{C_k}^2} \int_0^{2\pi} \int_0^{R_{C_k}} \frac{\Psi}{\Omega + \Psi + 1} r dr d\theta \right]. \tag{16}$$

*Remark 3:* The FD scheme will naturally lead to better performance, and this is reflected mathematically in the upper bound (15). Then for the FD scenario with fixed  $d_{i,i+1}$ , the SCP depends not only on the average number of eavesdroppers  $N_{C_k}$  in each representative cluster, but also on the related information of each cluster, i.e. the radius and location. Furthermore, the jamming power-to-noise ratio is also an important parameter, which can affect the SCP.

According to (5), the end-to-end enhanced SCP for the FD case can be given by

$$P^{(F)} = \prod_{i=1}^N P_i^{(F)}. \tag{17}$$

In Section VI, we will give the simulation results to verify the performance gain by using the FD receiver.

<sup>5</sup>The detail of SI cancellation for FD implementation is beyond the scope of this paper. More related details can be found at [36] and references therein.

<sup>6</sup>Note that the only difference between HD and FD is that the interference has to be received at the eavesdroppers, which is shown in the denominator of first line in (14).

$$\begin{aligned}
P_{co,i}^{(F)} &= \mathbb{P} \left( \frac{|h_{i,i+1}|^2 d_{i,i+1}^{-\alpha}}{\sum_{k=1}^K \sum_{e \in \Phi_{C_k}} \left( \frac{|h_{i,e}|^2 d_{i,e}^{-\alpha}}{\gamma_{C_k} |h_{i+1,e}|^2 d_{i+1,e}^{-\alpha} + 1} \right)} > 1 \right) = \prod_{k=1}^K \mathbb{E}_{e \in \Phi_{C_k}} \left[ \prod_{e \in \Phi_{C_k}} \exp \left( - \frac{d_{i,i+1}^\alpha d_{i,e}^{-\alpha} |h_{i,e}|^2}{\gamma_{C_k} |h_{i+1,e}|^2 d_{i+1,e}^{-\alpha} + 1} \right) \right] \\
&\stackrel{(a)}{=} \prod_{k=1}^K \mathbb{E}_{e \in \Phi_{C_k}} \left[ \prod_{e \in \Phi_{C_k}} \int_0^\infty e^{-l} f_L(l) dl \right] = \prod_{k=1}^K \mathbb{E}_{e \in \Phi_{C_k}} \left[ \prod_{e \in \Phi_{C_k}} \left( 1 - \frac{\Psi}{\Omega} \mathbb{E}_1 \left( \frac{\Psi+1}{\Omega} \right) e^{-\frac{\Psi+1}{\Omega}} \right) \right] \\
&\stackrel{(b)}{=} \prod_{k=1}^K \exp \left[ - \frac{N_{C_k}}{\pi R_{C_k}^2} \int_0^{2\pi} \int_0^{R_{C_k}} \left( \frac{\Psi}{\Omega} \mathbb{E}_1 \left( \frac{\Psi+1}{\Omega} \right) e^{-\frac{\Psi+1}{\Omega}} \right) r dr d\theta \right]
\end{aligned} \tag{14}$$

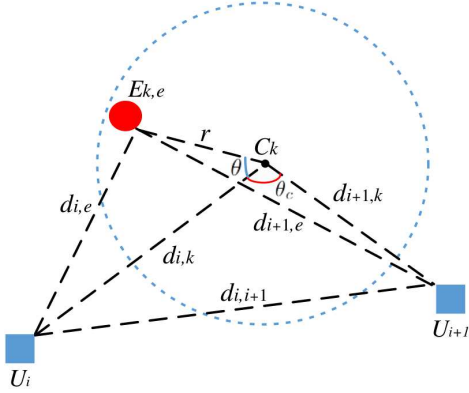


Figure 2. The relationship of distance among the  $U_i$ ,  $U_{i+1}$  and  $E_{k,e}$ .

## V. SECURE CONNECTIVITY ROUTING ALGORITHM

In the last Section, we provided the exact expressions of the SCP with the cases of half and full-duplex receiver under fixed eavesdropper clusters for a given path. According to the above results, the secure routing problem which is related to the optimal path selection to achieve the largest SCP from the source to the destination by utilizing multiple relays will be proposed in this section. Since we have the knowledge of eavesdropper clusters, in order to reduce the probability of eavesdropping, the relays located in eavesdropping clusters will be ignored. Before providing the routing algorithm, we give two simple metrics, which can be easily used to select the sub-optimal path.

### A. Two Metrics for Sub-Optimal Path Selection

1) *The central approximation:* When the average number of eavesdroppers and the locations of clusters are known, we can obtain a metric, which is termed the *central approximation*, to find the sub-optimal path from the transmitter to the receiver rather than the exact complex calculation of SCP. For the central approximation case, we consider all possible eavesdroppers located at the central point of their representative cluster. In other words, the legitimate transmitter is assumed to share an identical distance from all eavesdroppers, which are located in the same cluster as in [32]. Then the approximation of SCP between  $U_i$  and  $U_{i+1}$  with HD receiver is

$$P_i^{(C)} = \prod_{k=1}^K \exp \left[ -N_{C_k} \left( \frac{d_{i,k}^{-\alpha} d_{i+1,k}^{-\alpha}}{d_{i,k}^{-\alpha} d_{i+1,k}^{-\alpha} + 1} \right) \right]. \tag{18}$$

*Remark 4:* For given  $d_{i,i+1}$ , the SCP for the central approximation scenario is related to the average number of eavesdroppers and the locations of clusters. We can easily plug this result in the routing algorithm, which will be presented in the next subsection to find the sub-optimal path.

2) *The Mean Approximation:* For the mean approximation case, we derive the SCP between any two legitimate nodes with the mean of the sum SNRs of the eavesdroppers in the same cluster. First, we rewrite (7) as

$$P_i^{(M)} = \mathbb{P} \left( \frac{|h_{i,i+1}|^2 d_{i,i+1}^{-\alpha}}{\sum_{k=1}^K \mathbb{E} \left[ \sum_{e \in \Phi_{C_k}} (|h_{i,e}|^2 d_{i,e}^{-\alpha}) \right]} > 1 \right) \tag{19}$$

and we can obtain the mean approximation of SCP by the following lemma 2.

*Lemma 2:* The SCP between  $U_i$  and  $U_{i+1}$  with the mean of the sum of SNRs for eavesdropper is

$$P_i^{(M)} = \begin{cases} \exp \left( d_{i,i+1}^2 \sum_{k=1}^K \frac{N_{E_k}}{R_{C_k}^2} \ln \left( \frac{d_{i,k}^2}{d_{i,k}^2 - R_{C_k}^2} \right) \right) & \alpha = 2, \\ \exp \left( \sum_{k=1}^K \left( \frac{N_{E_k} d_{i,i+1}^4}{(R_{C_k}^2 - d_{i,k}^2)^2} \right) \right) & \alpha = 4. \end{cases} \tag{20}$$

*Proof:* See Appendix B. ■

### B. Routing Algorithm

Based on (6), we need to find the optimal route to achieve the maximum SCP<sup>7</sup>, which can be formulated as

$$\max_{\Pi \in S_{\Pi}} \prod_{i \in S_{\Pi}} P_i \tag{21}$$

where  $S_{\Pi}$  represents the set of all potential routes from the source to destination nodes. It is obviously demonstrated that this maximization problem may solved by using exhaustive search, however, this is a highly complex task. Therefore based on Dijkstra's algorithm, a novel route selection algorithm is proposed, which will provide the largest SCP from a source node to the destination node. For the random eavesdropper

<sup>7</sup>The proposed optimal route selection scheme can be achieved in a centralized or decentralized way. In the centralized algorithm, all route selections are made at a central node, while in the distributed algorithm, the computation of routes is shared among the network users with information exchanged between them as necessary. How to implement the centralized and distributed routing algorithms is beyond the scope of this paper. More details can be found in [38], [39].



**Algorithm 1** The routing algorithm for fixed cluster eavesdroppers scenario

**Input:** Network parameters setting  $[N_{C_k}, R_k, d_{i,i+1}, d_{i,k}]$  and  $d_{i+1,k}]$ ;

**Begin:**

- 1: Substitute the initial parameters into (11), (14), (19) and (20) to generate the adjacency SCP matrix ( $\mathbf{M} \in \mathcal{R}^{(N+2) \times (N+2)}$ ) for four route selection cases;
  - 2: Identify the source node ( $U_0$ ) and the destination node ( $U_{N+1}$ ) and set  $U_0$  as a permanent node;
  - 3: Let all other users as the temporary nodes;
  - 4: Search the temporary node with the largest SCP ( $\mathbf{M}(1, n)$ ) as  $U_n$  by utilizing  $n = \text{argmax}(\mathbf{M}(1, \mathbf{v}))$ , where  $\mathbf{v}$  denotes the index vector of the temporary nodes;
  - 5: Replace the SCP of temporary nodes by utilizing  $\mathbf{M}(1, \mathbf{v}) = \max(\mathbf{M}(1, \mathbf{v}), \mathbf{M}(1, n) \times \mathbf{M}(n, \mathbf{v}))$ ;
  - 6: Let  $U_n$  as a permanent node, then move to Step 4;
  - 7: When all temporary nodes are set as permanent nodes, the searching is finished;
- return**  $[\Xi^*, P(\Xi^*)]$ ;

clusters scenario, by substituting (9) into (21), we obtain the maximum SCP as

$$\max_{\Pi \in S_{\Pi}} \exp \left( - \frac{\pi \lambda_E \sum_{i \in S_{\Pi}} d_{i,i+1}^2}{\text{sinc}(\frac{2}{\alpha})} \right) \quad (22)$$

where the maximum SCP only depends on the distance between two legitimate nodes. Therefore, (22) is equivalent to

$$\min_{\Pi \in S_{\Pi}} \left( \sum_{i \in S_{\Pi}} d_{i,i+1}^2 \right). \quad (23)$$

It is clear that the problem can be easily addressed by using the classical shortest path selection algorithm<sup>8</sup>, i.e., Bellman-Ford and Dijkstra's algorithm.

For the fixed eavesdropper clusters, however, the optimal route selection depends on many factors, e.g., the radius and location of clusters, the average number of eavesdroppers, etc., which is different from the random eavesdropper clusters case. Therefore, at the beginning, each legitimate user has to obtain the distances between itself and all other legitimate nodes and the center points of the clusters in the network and saves the topology information, which includes the neighbor table, the radius of clusters and the average number of eavesdroppers in each cluster. Then by using the above analysis results (c.f., (11) and (14)) with topological knowledge, an adjacency SCP matrix ( $\mathbf{M} \in \mathcal{R}^{(N+2) \times (N+2)}$ ) can be obtained. Then we can find the optimal route with the largest SCP by utilizing the proposed routing Algorithm 1. It is clear that the computational complexity mainly depends on step 2 to 7, which is almost equivalent to the classical Dijkstra algorithm [42]. Therefore, the proposed algorithm has the same complexity of

<sup>8</sup>The classical shortest path selection algorithm can be easily found in the literature [40], [41], therefore, in our paper, we only focus on the routing algorithm for the fixed eavesdropper clusters case.

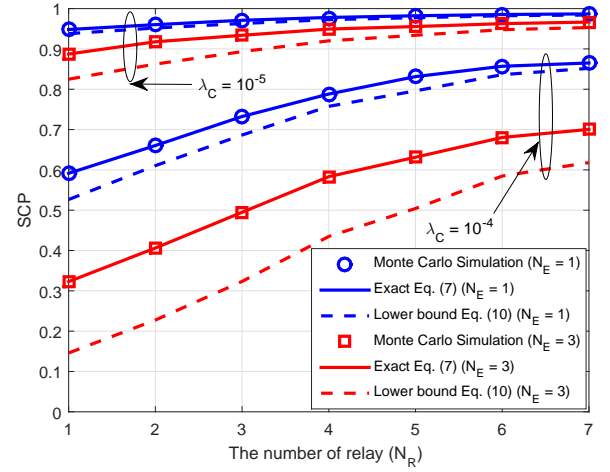


Figure 3. Theoretical v.s. numerical secrecy connectivity probabilities for random eavesdropper clusters with a given path.

computation compared to Dijkstra's algorithm  $\mathcal{O}(N^2)$ , which is much lower than the exhaustive search  $\mathcal{O}((N-2)!)$  [43].

## VI. SIMULATIONS

We give Monte Carlo (MC) simulation results to verify the above analysis in this section. The noise variance  $\sigma_n^2 = 1$  and the transmission-power-to-noise ratio  $P_B/\sigma_n^2 = 40$  dB are assumed, and the simulation results are given by averaging over  $10^5$  independent trials. The pathloss exponent is  $\alpha = 2$  and 4. We study two scenarios: one is the random eavesdropper clusters scenario and the other is the fixed eavesdropper clusters scenario. We choose the exhaustive search as a comparison benchmark to verify our proposed routing algorithm.

### A. Secrecy Performance Results for A Given Path

We verify the SCP of a given multi-hop wireless networks in this subsection. For example, the multi-hop networks with legitimate nodes  $U_0 \sim U_7$  which are located at  $(-20, 0)$ ,  $(-15, 5)$ ,  $(-10, 0)$ ,  $(-5, -2.5)$ ,  $(0, 0)$ ,  $(5, 5)$ ,  $(10, 0)$  and  $(20, 0)$  are investigated.

1) *Random eavesdropper clusters*: For random eavesdropper clusters, we assume that all of the clusters have the same radius and the average number of eavesdroppers. In Fig. 3, the comparison of SCP between the exact and lower bound result with different average number of eavesdroppers in each cluster and density of the cluster, where  $\alpha = 4$ , has been investigated. Both theoretical and simulation results are provided, which are match well. Moreover, we can see that the SCP increases with the increasing of number of hops (relays), which is a significant difference from DF relaying. The DF relays use the same codeword at the source and relay nodes, therefore, by increasing number of hops, the eavesdropper may catch the same information from different hops, so that the SCP will increase. In contrast, different codewords for RaF relaying have been used at the transmitter nodes, so that the more hops, the better the SCP when the locations of the relays are on the optimal path.

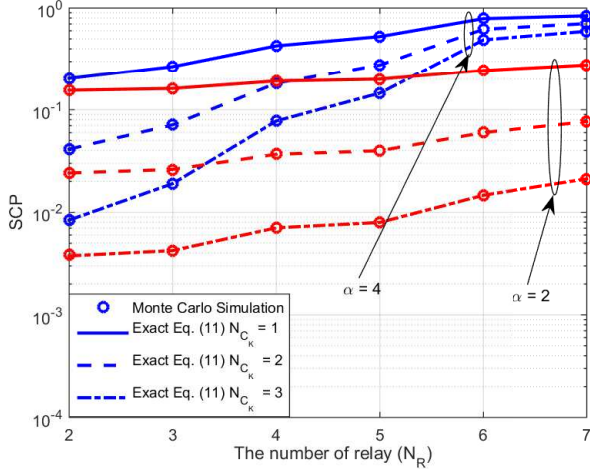


Figure 4. Theoretical v.s. numerical secrecy outage probabilities for the fixed eavesdropper clusters with a given path.

2) *Fixed eavesdropper clusters*: We assume the locations of eavesdropping clusters can be estimated at  $(-10, -30)$ ,  $(10, -30)$  and  $(0, 20)$  with the same radius 10 m for each cluster. Fig. 4 verifies the secrecy connectivity probabilities for a given path versus the different average number of eavesdroppers. The theoretical and simulation results match well. Moreover, we can see that the SCP increases when the number of relay nodes increases for both  $\alpha = 2$  and 4, due to the use of RaF relaying. Furthermore, the SCP decreases when the path loss exponent increases. Physically, this result shows that cluttered environments showing high propagation losses are more beneficial for security the same as in [28].

In order to improve the SCP, the FD receiver has been considered. In Fig. 5, the comparison of the SCP between the HD and FD receivers for different path loss exponents and jamming-power-to-noise ratios ( $P_J/\sigma_n^2$ ), where  $N_{C_1} = N_{C_2} = N_{C_3} = 3$ , have been studied. It is clearly shown that compared to the HD receiver, the SCP with the FD receiver will increase when the jamming-power-to-noise ratio increases. Furthermore, in the cluttered environments, i.e.,  $\alpha = 4$ , more energy in the jamming signal will be required than for free space ( $\alpha = 2$ ) to achieve a certain SCP.

### B. Performance of Path Selection

We consider a multi-hop wireless network where the relay nodes ( $N_R = 20$ ) are uniformly located<sup>9</sup> in a  $100 \times 100$  m<sup>2</sup> square area in this subsection. The locations of source and destination are  $(-50, 0)$  and  $(50, 0)$ , respectively. Moreover, the locations of four eavesdropper clusters ( $C_1, C_2, C_3$  and  $C_4$ ) are fixed at  $(-30, -30)$ ,  $(-20, 30)$ ,  $(10, -15)$  and  $(30, -5)$  with different radii ( $R_{C_1} = 20$  m,  $R_{C_2} = 10$  m,  $R_{C_3} = 10$  m and  $R_{C_4} = 5$  m).

In Fig. 6, the comparison of the secure path for the different selected metrics in a snapshot of the network are given, where  $\alpha = 4$  and  $N_{C_1} = N_{C_2} = N_{C_3} = N_{C_4} = 1$ . It is clear from these results that the proposed exact route (c.f. (11)), the central

<sup>9</sup>We have chosen randomly the locations of relays, but then fixed these for the duration of the simulation study as a snapshot.

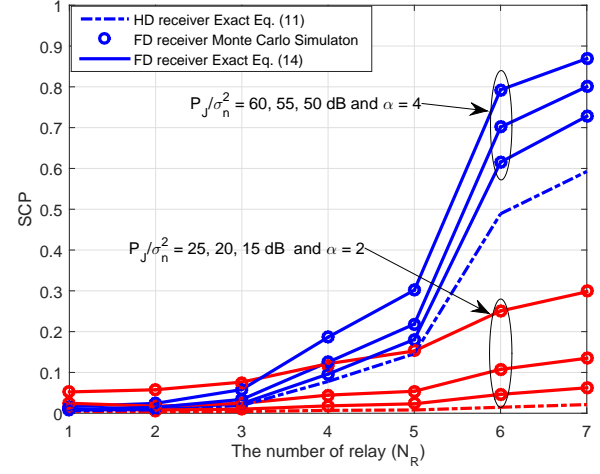


Figure 5. The comparison of SCP between HD and FD receiver for different jamming power-to-noise ratios, where  $N_{C_1} = N_{C_2} = N_{C_3} = 3$ .

Table II  
THE COMPARISON OF END-TO-END SCP FOR THE DIFFERENT SELECTED METRICS.

	$N_{C_k} = 10^{-2}$	$N_{C_k} = 10^{-1}$	$N_{C_k} = 1$
Exhaustive search	0.9741	0.7679	0.0708
Exact	0.9738	0.7670	0.0705
Central app.	0.9739	0.7672	0.0706
Mean app.	0.9699	0.7370	0.0473

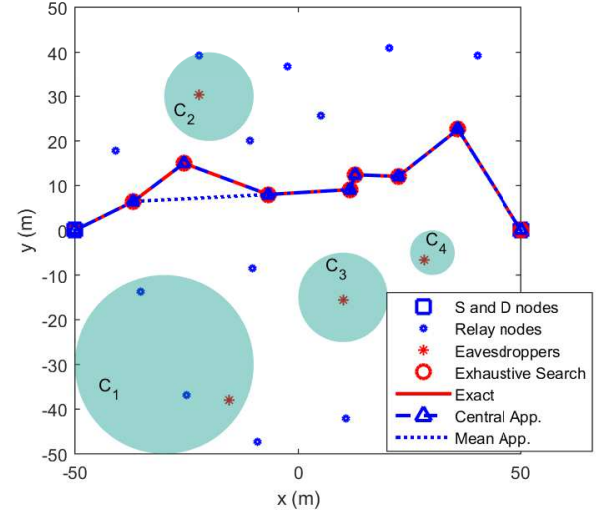


Figure 6. The comparison of the secrecy path for the different selected metrics in a snapshot of the network, where  $\alpha = 4$  and  $N_{C_1} = N_{C_2} = N_{C_3} = N_{C_4} = 1$ .

approximation route (c.f. (20)) and the mean approximation route (c.f. (19)) are close to the benchmark route. We also give Table II to compare the end-to-end SCP for different cases. It is shown that the SCP of the proposed schemes are similar with the exhaustive search.

Fig. 7 shows the effect of different average numbers of eavesdroppers for the optimal route in a snapshot of the network, where  $\alpha = 4$ . Again, the theoretical results gen-



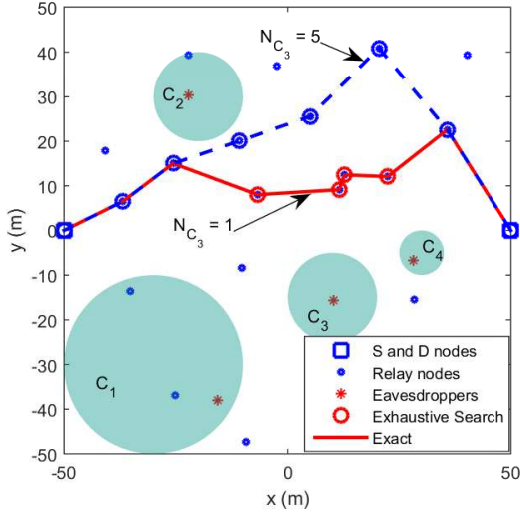


Figure 7. The effect of different average numbers eavesdroppers on the optimal route in a snapshot of the network, where  $\alpha = 4$ .

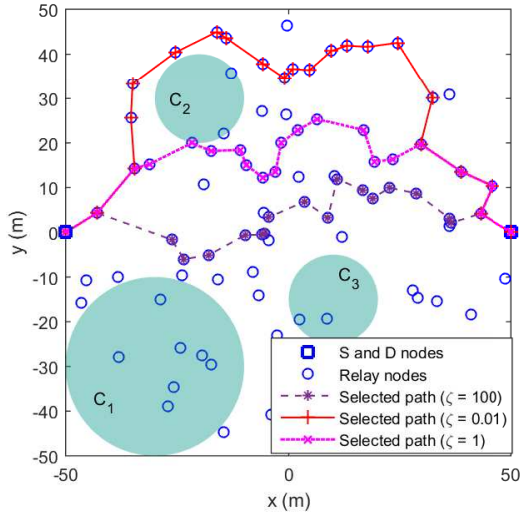


Figure 8. The effect of different estimated error ratio for optimal route in a snapshot of the network, where  $\alpha = 4$ .

erated by (11) are matched to the MC simulation results. Furthermore, if let  $N_{C_1} = N_{C_2} = N_{C_4} = 1$ , it is shown that the optimal path changes when the  $N_{C_3}$  increases from 1 to 5, because the distant node needs to be selected to avoid being eavesdropped. By doing so, when we can estimate the locations and radii of the eavesdropper clusters and the average number of eavesdroppers, an optimal path can be designed to obtain the largest SCP.

In fact, the area of the eavesdropping cluster may be easily measured, due to the geographical limitations (i.e., in the specified building or area). However, the average number of eavesdroppers is normally difficult to be estimated accurately. Therefore, we give an example to discuss how the estimated error of the average number of eavesdroppers affects secrecy connectivity performance. Here, we only give the theoretical results of SCP, because the complexity of computation of the exhaustive search is high. Fig. 8 provides the selected path changes for a snapshot of the network, where 100 relays are

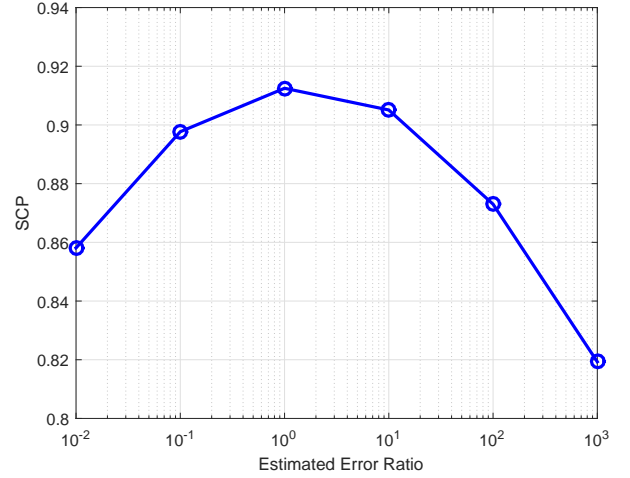


Figure 9. The SCP v.s. the estimated error ratio.

uniformly located at  $100 \times 100 \text{ m}^2$  square area according to different estimated error ratios. We assume the accurate average number of eavesdroppers in cluster 3 ( $C_3$ ) is  $N_{C_3} = 1$  with the radius ( $R_{C_3} = 10 \text{ m}$ ), and fix the average numbers of cluster 1 and 2, which are the same ( $N_{C_1} = N_{C_2} = 0.1$ ) and the radius of  $C_1$  and  $C_2$  as 20 and 10 m, respectively. We define the estimated error ratio as

$$\zeta = \frac{N_C^{(A)}}{N_C^{(E)}} \quad (24)$$

where  $N_C^{(A)}$  and  $N_C^{(E)}$  denote the accurate and estimated average number of eavesdroppers in the cluster, respectively. It is shown that when the estimated error ratio is small, i.e.,  $\zeta = 0.01$ , which means the number of eavesdroppers is estimated to be high, the selected path is far away from cluster 3. In contrast, when the estimated error ratio is large, the selected path is close to cluster 3. In order to give a clear comparison of the effects on SCP, we provide Fig. 9, which shows how the estimated error of the average number of eavesdroppers affects the SCP. It is clearly shown that when the estimated average number of eavesdroppers is the same as the accurate average number of eavesdroppers ( $\zeta = 1$ ), we can achieve the maximum SCP, otherwise, the SCP decreases.

## VII. CONCLUSION

This work studied optimal secure routing based on the SCP in multi-hop ad hoc networks with RaF relaying in the presence of inhomogeneous eavesdropper clusters. Both fixed and random locations of the eavesdropper clusters have been investigated. Furthermore, the end-to-end SCP for any given path in general multi-hop wireless networks with HD RaF relays has been derived. An FD scheme at the legitimate receiver has been utilized to further enhance the secrecy connectivity. Moreover, a novel secure routing algorithm has been proposed, which can achieve the maximum SCP between legitimate transmitter and receiver in a distributed manner. Finally, we used MC simulations to verify the derived theoretical results. According to the simulations, for the random eavesdropper clusters case, the optimal route selection is independent from

the locations of the cluster, which is the same as the homogeneous eavesdropper case. However, for the fixed eavesdropper clusters case the analysis shown that the optimal route relates on the locations and radii of eavesdropper clusters and the average number of eavesdroppers.

#### APPENDIX A - PROOF OF Lemma 1

According to (7), for the random clustered process, the SCP is derived by

$$P_{co,i}^{(E)} = \mathbb{P} \left( \frac{|h_{i,i+1}|^2 d_{i,i+1}^{-\alpha}}{\sum_{k=1}^K \sum_{e \in \Phi_{C_k}} (|h_{i,e}|^2 d_{i,e}^{-\alpha})} > 1 \right) \quad (25)$$

$$= \exp \left[ -\lambda_C \int_{\mathbb{R}^2} [1 - \exp(-N_E \xi(d_{i,i+1}, d_{i,k}))] dx_c \right]$$

where

$$\xi(d_{i,i+1}, d_{i,k}) = \int_{\mathbb{R}^2} \frac{f(x_e)}{1 + d_{i,i+1}^\alpha d_{i,e}^{-\alpha}} dx_e \quad (26)$$

and  $d_{U_i E_k} = \sqrt{d_{i,k}^2 + x_e^2 - 2\cos(\theta)x_e d_{i,k}}$ . Then we can obtain the lower bound of (25) as

$$\begin{aligned} P_{co,i}^{(E)} &\stackrel{(a)}{\geq} \exp \left[ -\lambda_E \int_{\mathbb{R}^2} \xi(d_{i,i+1}, d_{i,k}) dx_c \right] \\ &\stackrel{(b)}{=} \exp \left[ -\lambda_E \int_{\mathbb{R}^2} \frac{d_{i,k}^\alpha}{d_{i,i+1}^\alpha + d_{i,k}^\alpha} dx_c \right] \\ &\stackrel{(c)}{=} \exp \left( -\pi \lambda_E \frac{d_{i,i+1}^2}{\text{sinc}(2/\alpha)} \right) \end{aligned} \quad (27)$$

where (a) is the result of  $\exp(-ax) \geq 1 - ax$  for  $a \geq 0$ ; (b) holds from changed of variables, interchanging integrals and utilizing  $\int f(x)dx = 1$ ; (c) denotes the SCP of Neyman-Scott cluster processes is lower than the Poisson process of the same intensity as given in [10]. This concludes the proof.

#### APPENDIX B - PROOF OF Lemma 2

According to (19), we define  $S = \sum_{e \in \Phi_{C_k}} \left( \frac{|h_{i,e}|^2}{d_{i,e}^\alpha} \right)$  and by using Campbell's theorem, if  $\Phi_{C_k} \subset \mathbb{R}^2$  is stationary, the sum  $S$  is a R.V. with mean

$$\begin{aligned} \mathbb{E}(S) &= \frac{N_E}{\pi R_{C_k}^2} \int_0^{2\pi} \int_0^{R_{C_k}} \frac{r}{\sqrt{d_{i,k}^2 + r^2 - 2rd_{i,k}\cos(\theta)}}^\alpha dr d\theta \\ &= \begin{cases} \frac{N_E k}{R_{C_k}^2} \ln \left( \frac{d_{i,k}^2}{d_{i,k}^2 - R_{C_k}^2} \right) & \alpha = 2, \\ \frac{N_E k d_{i,k}^2}{R_{C_k}^2 (d_{i,k}^2 - R_{C_k}^2)^2} & \alpha = 4. \end{cases} \end{aligned} \quad (28)$$

Then, the CDF of  $|h_{i,i+1}|^2$  is  $F(x) = 1 - \exp(-x)$ . Therefore, we can obtain the SCP based on the mean approximation as given in (20). This concludes the proof.

#### REFERENCES

- [1] Y. Zhang, L. Song, C. Jiang, N. H. Tran, Z. Dawy, and Z. Han, "A social-aware framework for efficient information dissemination in wireless ad hoc networks," *IEEE Commun. Mag.*, vol. 55, pp. 174–179, Jan. 2017.
- [2] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017.
- [3] E. D. Silva, A. L. D. Santos, L. C. P. Albin, and M. Lima, "Identity based key management in mobile ad hoc networks: Techniques and applications," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 46–52, Oct. 2008.
- [4] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inform. Forensics and Security*, vol. 10, no. 3, pp. 574–583, Apr. 2015.
- [5] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
- [6] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Inf. Theory, Toronto, Canada*, pp. 539–543, July 2008.
- [7] P. C. Pinto, J. Barros, and M. Z. Win, "Physical-layer security in stochastic wireless networks," in *Proc. IEEE Int. Conf. Commun. Syst., Guangzhou, China*, pp. 974–979, Nov. 2008.
- [8] Y. J. Chun, M. O. Hasna, and A. Ghrayeb, "Modeling heterogeneous cellular networks interference using poisson cluster processes," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 10, pp. 2182–2195, Oct. 2015.
- [9] V. Suryaprakash, J. Miller, and G. Fettweis, "On the modeling and analysis of heterogeneous radio access networks using a poisson cluster process," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1035–1047, Feb. 2015.
- [10] R. K. Ganti and M. Haenggi, "Interference and outage in clustered wireless ad hoc networks," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4067–4086, Sep. 2009.
- [11] C. H. Liu, B. Rong, and S. Cui, "Optimal discrete power control in poisson-clustered ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 138–151, Jan. 2015.
- [12] Y. Wang and Q. Zhu, "Modeling and analysis of small cells based on clustered stochastic geometry," *IEEE Communications Letters*, vol. 21, no. 3, pp. 576–579, March 2017.
- [13] J. G. Andrews, R. K. Ganti, M. Haenggi, N. Jindal, and S. Weber, "A primer on spatial modeling and analysis in wireless networks," *IEEE Communications Magazine*, vol. 48, no. 11, pp. 156–163, Nov. 2010.
- [14] Y. Zhong and W. Zhang, "Multi-channel hybrid access femtocells: A stochastic geometric analysis," *IEEE Transactions on Communications*, vol. 61, no. 7, pp. 3016–3026, July 2013.
- [15] M. Afshang and H. S. Dhillon, "Spatial modeling of device-to-device networks: Poisson cluster process meets poisson hole process," in *49th Asilomar Conference on Signals, Systems and Computers*, pp. 317–321, Nov. 2015.
- [16] I. Krikidis, J. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.
- [17] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Processing*, vol. 58, pp. 1875–1888, March 2010.
- [18] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, pp. 878–881, June 2012.
- [19] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE Journal on Selected Areas in Commun.*, vol. 30, pp. 359–368, February 2012.
- [20] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Processing*, vol. 62, pp. 2185–2199, May 2014.
- [21] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inform. Forensics and Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.
- [22] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Transactions on Wireless Communications*, vol. 10, pp. 2764–2775, Aug. 2011.
- [23] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. on Wireless Commun.*, vol. 13, pp. 2931–2943, May 2014.
- [24] T. X. Zheng, H. M. Wang, and Q. Yin, "On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers," *IEEE Commun. Lett.*, vol. 18, pp. 1299–1302, Aug. 2014.

- [25] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a poisson random field of eavesdroppers," in *Proc. IEEE ICC*, Kyoto, Japan, June 2011.
- [26] T. X. Zheng, H. M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. on Commun.*, vol. 63, pp. 4347–4362, Nov. 2015.
- [27] G. Chen, J. P. Coon, and M. D. Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics and Security*, vol. 12, pp. 1195–1206, May 2017.
- [28] G. Chen and J. P. Coon, "Secrecy outage analysis in random wireless networks with antenna selection and user ordering," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 334–337, June 2017.
- [29] S. Cho, G. Chen, and J. P. Coon, "Securing visible light communication systems by beamforming in the presence of randomly distributed eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 17, no. 5, pp. 2918–2931, May 2018.
- [30] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks," *IEEE Journal on Selected Areas in Commun.*, vol. 36, no. 1, pp. 162–174, Jan. 2018.
- [31] W. Saad, X. Zhou, B. Maham, T. Basar, and H. V. Poor, "Tree formation with physical layer security considerations in wireless multi-hop networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3980–3991, Nov. 2012.
- [32] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, vol. 64, pp. 753–764, Feb. 2016.
- [33] S. Hong, J. Brand, J. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis, "Applications of self-interference cancellation in 5G and beyond," *IEEE Commun. Magazine*, vol. 52, no. 2, pp. 114–121, Feb. 2014.
- [34] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, pp. 3000–3015, May 2012.
- [35] M. Haenggi, "Stochastic geometry for wireless networks," *Cambridge Univ. Press*, 2012.
- [36] B. Debaillie, D. J. van den Broek, C. Lav, B. van Liempd, E. A. M. Klumperink, C. Palacios, J. Craninckx, B. Nauta, and A. Pssinen, "Analog/RF solutions enabling compact full-duplex radios," *IEEE Journal on Selected Areas in Commun.*, vol. 32, no. 9, pp. 1662–1673, Sep. 2014.
- [37] M. Abramowitz and I. A. Stegun, "Handbook of mathematical functions: with formulas, graphs, and mathematical tables," *Courier Corporation*, 1964.
- [38] Pierre A. Humblet, "An adaptive distributed Dijkstra shortest path algorithm," tech. rep., Technical Report CICSP-60, Center for Intelligent Control System, MIT, May 1988.
- [39] D. P. Bertsekas and R. G. Gallager, *Data networks*. Englewood Cliffs, NJ, USA: Prentice-Hall, Inc, 2 ed., 1992.
- [40] D. E. Knuth, "A generalization of Dijkstra's algorithm," *Information Processing Letters*, vol. 6, no. 1, pp. 1–5, Feb. 1997.
- [41] J. Y. Yen, "An algorithm for finding shortest routes from all source nodes to a given destination in general networks," *Quarterly of Applied Mathematics*, vol. 27, pp. 526–530, 1970.
- [42] G. Chen, J. Tang, and J. P. Coon, "Optimal routing for multihop social-based D2D communications in the internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1880–1889, June 2018.
- [43] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *IEEE WMCSA Workshop*, New Orleans, USA, Feb. 1999.



**Gaojie Chen** (S'09 – M'12) received the B.Eng. and B.Ec. degrees in electrical information engineering and international economics and trade from Northwest University, China, in 2006, and the M.Sc. (Hons.) and Ph.D. degrees in electrical and electronic engineering from Loughborough University, Loughborough, U.K., in 2008 and 2012, respectively. From 2008 to 2009, he was a Software Engineering with DTmobile, Beijing, China, and from 2012 to 2013, he was a Research Associate with the School of Electronic, Electrical and Systems Engineering, Loughborough University. He was a Research Fellow with 5GIC, Faculty of Engineering and Physical Sciences, University of Surrey, U.K., from 2014 to 2015. Then he was a Research Associate with the Department of Engineering Science, University of Oxford, U.K., from 2015 to 2018. He is currently a Lecturer with the Department of Engineering, University of Leicester, U.K. His current research interests include information theory, wireless communications, cooperative communications, cognitive radio, secrecy communication, and random geometric networks.



**Justin P. Coon** (S'02 – M'05 – SM'10) received the B.Sc. degree (Hons.) in electrical engineering from the Calhoun Honours College, Clemson University, USA, and the Ph.D. degree in communications from the University of Bristol, U.K., in 2000 and 2005, respectively. In 2004, he joined as a Research Engineer with the Bristol-based Telecommunications Research Laboratory (TRL), Toshiba Research Europe Ltd., where he was involved in research on a broad range of communication technologies and theories, including single- and multi-carrier modulation techniques, estimation and detection, diversity methods, and system performance analysis and networks. He held the research manager position from 2010 to 2013, during which time he led all theoretical and applied research on the physical layer at TRL. He was a Visiting Fellow with the School of Mathematics, University of Bristol, from 2010 to 2012, where he held a reader position with the Department of Electrical and Electronic Engineering from 2012 to 2013. He joined the University of Oxford in 2013, where he is currently an Associate Professor with the Department of Engineering Science and a Tutorial Fellow of Oriel College.

He is the Technical Manager of the EU FP7 project DIWINE. He has authored in excess of 100 papers in leading international journals and conferences, and is a named inventor on over 30 patents. His research interests include communication theory, information theory, and network theory. Dr Coon was a recipient of TRL's Distinguished Research Award for his work on block-spread CDMA, aspects of which have been adopted as mandatory features in the 3GPP LTE Rel-8 standard. He was also a co-recipient of two best paper awards at the ISWCS 2013 and the EuCNC 2014. He received the award for Outstanding Contribution in 2014. He has served as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2007 to 2013, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY from 2013 to 2016. He has been serving as an Editor for the IEEE WIRELESS COMMUNICATIONS LETTERS since 2016 and the IEEE COMMUNICATIONS LETTERS since 2017.



**Shahriar Etemadi Tajbakhsh** received a B.Sc in electrical engineering and a M.Sc in information technology engineering from Shahid Bahonar University of Kerman and Sharif University of Technology in 2006 and 2009 respectively. He finished his PhD in engineering at the Australian National University in 2014 followed by postdoctoral research studies at University of New South Wales and University of Oxford. Recently he has joined the University of Sussex and Moogsoft as a knowledge transfer partnership associate.